



# **TASK ORDER (TO)**

47QFCA21F0057

## **Decisive Action**

in support of:

## **Defense Threat Reduction Agency (DTRA)**



**Awarded To:**

**CACI NSS, LLC (CACI)  
14370 Newbrook Drive  
Chantilly, VA 20151**

**Conducted under Federal Acquisition Regulation (FAR) 16.505**

**Issued by:**

**The Federal Systems Integration and Management Center (FEDSIM)  
1800 F Street, NW (QF0B)  
Washington, D.C. 20405**

**June 25, 2021**

**FEDSIM Project Number 47QFCA21Z1110**

## SECTION C - PERFORMANCE WORK STATEMENT

### **C.1 BACKGROUND**

The Defense Threat Reduction Agency (DTRA) is a combat support agency that enables the Department of Defense (DoD), U.S. Government, and international partners to counter and deter Weapons of Mass Destruction (WMD) and improvised threat networks. DTRA is the DoD's leader for targeted WMD and improvised threat Research and Development (R&D), and it facilitates innovation to develop and quickly field solutions to the most complex, deadly, and urgent threats in the world. DTRA began strictly as a weapons development program in 1942 as part of the Manhattan Project called the Defense Special Weapons Agency; it expanded during the Cold War to eventually include non-nuclear weapons development and nonproliferation efforts. In November 1997, the Defense Reform Initiative merged the Defense Special Weapons Agency and the On-Site Inspection Agency with two defense programs – the Cooperative Threat Reduction (CTR) Program and the Chemical-Biological Defense Program, Science, and Technology component. These programs formed the core elements of DTRA.

DTRA was formally established on October 1, 1998. As threats continued to evolve, the DoD also established the Joint Improvised Explosive Device Defeat Organization (JIEDDO) in 2006 to lead and coordinate the DoD's Counter-Improvised Explosive Device (C-IED) efforts. Since 2006, the nature, scope, and use of improvised threat devices significantly evolved and increased in lethality and accessibility to the enemy. These threats now come from state actors, terrorist groups, enemy combatants, and widely divergent improvised threat networks.

In 2015, the Deputy Secretary of Defense expanded JIEDDO's mission from solely countering/defeating Improvised Explosive Devices (IEDs) to countering and defeating improvised threats at large. With this expanded mission, the name of the organization changed to the Joint Improvised Threat Defeat Organization (JIDO), and JIDO was ultimately re-aligned under DTRA in 2016. The JIDO functions have been fully integrated with DTRA, and the JIDO name has been retired.

As used in this document, WMD are defined as follows:

Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high-yield explosives or nuclear, biological, chemical, or radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. (Joint Publication 1-02)

As used in this document Improvised Threats are defined as follows:

Devices, systems, and associated Tactics, Techniques, and Procedures (TTPs) designed, fielded or employed unconventionally that are intended to adversely impact U.S. and coalition forces.

The term deployment used in this document refers to extended Temporary Duty (TDY) in Hazardous Duty/Combat Zones (HD/CZ) (e.g., Afghanistan).

## SECTION C - PERFORMANCE WORK STATEMENT

### **C.1.1 PURPOSE**

The purpose of this Decisive Action (DA) Task Order (TO) is to provide a wide range of professional analytical services to assist DTRA with its mission of countering and deterring WMD, improvised threats, and threat networks in the Continental United States (CONUS) and OCONUS. The efforts performed under the DA TO will enhance DTRA's situational understanding of threat networks and support Combatant Commands (CCMDs) with the integration of analysis, capabilities, technologies, and lessons learned to defeat the enemy networks that employ improvised threat weapons and WMD for strategic effect.

### **C.1.2 AGENCY MISSION**

DTRA is a combat support agency that enables the DoD, U.S. Government, and international partners to counter and deter WMD and improvised threat networks. DTRA is the DoD's leader for targeted WMD and improvised threat R&D and facilitates innovation to develop and quickly field solutions to the most complex, deadly, and urgent threats in the world. DTRA's mission is three pronged:

- a. To counter the threats posed by the full spectrum of WMD including Chemical, Biological, Radiological, Nuclear, and high-yield Explosives (CBRNE).
- b. To counter threats posed by the growing, evolving categories of improvised threats including IEDs and car bombs as well as the tactics, technologies, and networks that put them on the battlefield.
- c. To ensure the U.S. military maintains a safe, secure, effective, and credible nuclear weapon deterrent.

### **C.2 SCOPE**

The scope of the DA TO is to provide integrated operations analysis services to DTRA and its supported CCMDs for the purpose of countering and deterring WMD and threat networks. Contractor analysts may be embedded with U.S. Forces, or be required to deploy to an OCONUS theater of operations, sometimes within a HD/CZ. The services provided by the contractor may support theater peacetime, crisis, and contingency operations.

The required services are provided primarily at the DTRA facility in the National Capital Region (NCR); however, support is also anticipated at other CONUS and OCONUS locations.

### **C.3 CURRENT ENVIRONMENT**

Unpredictable world events demand that DTRA have the capability to provide critical analytical support anywhere in the world. This support may include deployments that are variable in length and rotational deployments that are short-term (e.g., one month or less) or long-term (e.g., four to six months). While areas of performance may be identified during the base period of performance, it is impossible to predict the precise need and nature of required services because they fluctuate in response to world events.

## SECTION C - PERFORMANCE WORK STATEMENT

DTRA has an internal process for providing analysis reports called the Request for Support (RFS). A key ingredient of the RFS process is delivery of the requested support within the time frame identified on the RFS. The information provided in the RFS analysis is only as good as the time frames within which it is provided. If the information or analysis is provided after the due date specified in the RFS, it is of no value to decision makers. This process is further described in **Section C.5.4.3**.

### **C.4 OBJECTIVE**

DTRA combats rapidly changing threats; therefore, DTRA must be agile and flexible in order to assess and respond to internal demands and external inquiries. Worldwide operations drive DTRA to pursue a more capable execution framework. The overarching objective for the TO is to have improvements to processes that will drive operating efficiencies and ultimately result in flexible and agile response to requirements. The contractor shall be responsible for delivering highly specialized expertise in order to meet this objective. Other goals of this effort include, but are not limited to:

- a. Identification of innovative solutions for improving workflow processes (i.e., automation of deliverables).
- b. Identification of efficiencies or improvements to mission effectiveness.
- c. Innovations for deployment tracking (for classified/unclassified).
- d. Identification of improvements/innovations to quality control efforts.
- e. Identification of cost saving/cost avoidance measures.

### **C.5 TASKS**

The contractor shall perform the following tasks in support of this TO:

- a. Task 1 – Provide Program Management
- b. Task 2 – Planning, Strategy, and Engagement Support
- c. Task 3 – Operational Effects (OPX), Special Access Programs (SAP) Integration
- d. Task 4 – Provide Liaison, Integration, and Weapons Technical Intelligence (WTI) Support
- e. Task 5 – Analytical Support
- f. Task 6 – Specialized Analysis
- g. Task 7 – Pattern Analysis/Technical Support
- h. Task 8 – Operations Research/Systems Analysis (ORSA)
- i. Task 9 – Joint Expeditionary Team (JET)
- j. Task 10 – Optional Surge

#### **C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT**

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS.

## SECTION C - PERFORMANCE WORK STATEMENT

The contractor shall identify a Program Manager (PM) to serve as the primary interface and Point of Contact (POC) with the FEDSIM Contracting Officer's Representative (COR) and the DTRA Technical Point of Contact (TPOC). The contractor PM shall be responsible for managing and overseeing the activities of all contractor personnel as well as subcontractor and teaming partners. Additionally, the contractor PM shall provide management, direction, administration, quality assurance, and leadership execution of this TO.

The contractor shall institute and maintain industry best practices, standards, processes, and methodologies. The contractor shall immediately notify the FEDSIM COR and DTRA TPOC if it encounters any technical, security, financial, personnel, or general managerial problems throughout the TO performance (**See Section C.5.1.4 Problem Notification Report**).

### **C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING**

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DTRA as directed by the FEDSIM CO. The secure data collection site, System for Award Management (SAM) will be utilized for reporting contractor labor. The contractor shall completely fill in all required data fields using the SAM: <https://sam.gov/SAM/pages/public/index.jsf>.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the SAM support desk at: <https://www.fsd.gov/fsd-gov> or telephonically at 866-606-8220.

### **C.5.1.2 SUBTASK 2 – COORDINATE A PROGRAM KICK-OFF MEETING**

The contractor shall schedule, coordinate, and host a Program Kick-Off Meeting at the location approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the contractor's Key Personnel, the DTRA TPOC, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR.

At least three days prior to the Program Kick-Off Meeting, the contractor shall provide a **Program Kick-Off Meeting Agenda and Presentation Slides (Section F, Deliverable 1)** for review and approval by the FEDSIM COR and the DTRA TPOC prior to finalizing. The agenda and slides shall include, at a minimum, the following topics/deliverables:

- a. Introduction of POCs for all parties.
- b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
- c. Project Staffing Plan and status.
- d. Transition discussion.

## SECTION C - PERFORMANCE WORK STATEMENT

- e. Program Management Plan (PMP) content discussion (including schedule and tasks) and status.
- f. Quality Management Plan (QMP) content discussion.
- g. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
- h. Financial forecasting/tracking and invoicing requirements (**Section C.5.1.10**).
- i. TO Portal Strategy and Demonstration (**Section C.5.1.9**).

The Government will provide the contractor with the number of Government participants for the Program Kick-Off Meeting, and the contractor shall provide copies of the presentation for all present.

The contractor shall draft and provide a **Program Kick-Off Meeting Minutes (Section F, Deliverable 2)** documenting the Program Kick-Off Meeting discussion and capturing any action items.

### **C.5.1.3 SUBTASK 3 – PREPARE A MONTHLY STATUS REPORT (MSR)**

The contractor shall develop and provide an **MSR (Section J, Attachment E) (Section F, Deliverable 3)**. The MSR shall include the following:

- a. For each task/project, the activities during the reporting period and/or completed during the previous month (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section should start with a brief description of the task.
- b. Identify issues or concerns and corrective actions taken or proposed (depending on status).
- c. Updated personnel roster that includes all contractor personnel (including subcontractors and teaming partners) by location, project, OASIS LCAT Personnel gains, losses, and status (security clearance, etc.).
- d. Government actions required.
- e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
- g. Financial Status:
  - 1. Costs incurred at the CLIN and project level, broken out by prime contractor, subcontractor(s), and teaming partner(s) through the previous month.
  - 2. Costs invoiced at the CLIN level and project level, broken out by prime contractor, subcontractor(s), and teaming partner(s) through the previous month.
  - 3. Projected costs to be incurred at the CLIN and project level, broken out by prime contractor, subcontractor(s), and teaming partner(s) for the current month.

## SECTION C - PERFORMANCE WORK STATEMENT

- h. List of deliverables provided (identify deliverable title, number, location, and date of approval). If the deliverable is classified, the contractor shall develop a numbering/identification scheme.
- i. Recommendations for improvements, changes, or modifications to tasks or processes that would result in efficiencies.

### **C.5.1.4 SUBTASK 4 – PROBLEM NOTIFICATION REPORT (PNR)**

The contractor shall notify the FEDSIM COR via the **PNR Template (Section J, Attachment F) (Section F, Deliverable 4)** as soon as it becomes apparent to the contractor that a problem will occur (i.e., a scheduled delivery will be late, or a cost overrun will occur). The contractor shall include in the PNR the rationale for the problem (e.g., why it occurred), identify the overall impact of the problem to the TO, and provide a mitigation strategy. The FEDSIM COR will review the PNR and provide guidance to the contractor. Such notification in no way limits the Government's contractual rights or remedies including, but not limited to, termination.

### **C.5.1.5 SUBTASK 5 – CONVENE TECHNICAL STATUS/TECHNICAL MEETINGS**

The contractor PM shall facilitate and participate in regular technical status/project meetings. The contractor shall provide technical status/project briefings to the FEDSIM COR and DTRA TPOC.

In addition to technical status/project meetings, the contractor PM shall ensure the appropriate representation for all technical meetings, working groups, interchange meetings, and integrated program management reviews. The contractor shall develop **Meeting Presentation Materials/Briefings (Section F, Deliverable 5)**. The contractor shall document and provide to the Government the **Technical Status/Project Meeting Minutes (Section F, Deliverable 6)** for each technical status/project meeting that includes, at a minimum, the following information:

- a. Meeting attendees and their contact information/organization.
- b. Meeting date and location.
- c. Meeting agenda.
- d. Purpose of the meeting.
- e. Discussion of any unresolved action items from the previous meeting with a status and date of the associated meeting.
  - 1. Identification of the resolution or proposed resolutions to the unresolved actions.
- f. Summary of what transpired (issues and risks discussed, decisions made, action items, and the identification of the individual responsible for action items).
- g. Conclusion and recommendations of the meeting.
- h. Next scheduled event(s) impacting or impacted by the meeting.

#### **C.5.1.5.1 SUBTASK 5.1 – INTEGRATED PROGRAM REVIEWS (IPR)**

The contractor shall provide a TO status update during DTRA's monthly IPR. This status update shall be provided to the FEDSIM COR, DTRA TPOC, and other Government stakeholders. In

## SECTION C - PERFORMANCE WORK STATEMENT

support of the IPR, the contractor shall develop and **provide briefings (Section F, Deliverable 5)** to describe financial status and specific initiatives, both ongoing and completed, throughout the period of performance. The contractor shall take **minutes** at the **IPRs (Section F, Deliverable 6)** in accordance with **Section C.5.1.5**.

### **C.5.1.6 SUBTASK 6 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)**

The contractor shall prepare a **PMP (Section F, Deliverable 7)** and provide it to the Government. The PMP shall provide an overall plan for the TO and, at a minimum, shall:

- a. Describe the proposed management approach.
- b. Contain detailed Standard Operating Procedures (SOPs) for all tasks that require Government involvement and/or approval.
- c. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
  1. The WBS shall identify all technical activities at a level of detail sufficient for the contractor to manage the work.
  2. Each WBS element shall be accompanied by a description and expected result(s).
  3. Each WBS element shall include an estimate of the Level of Effort (LOE) required by LCAT and associated cost.
- d. Include an Integrated Master Schedule with the milestones, tasks, and subtasks required in this TO.
- e. Describe in detail the contractor's approach to risk management under this TO.
- f. Describe in detail the contractor's approach to communications, including processes, procedures, format, and other rules of engagement between the contractor and the Government.

The PMP is an evolutionary document that shall be updated annually at a minimum and as project changes occur. The contractor shall work from the latest Government-approved version of the PMP.

### **C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS**

The Government will require a **Trip Report (Section F, Deliverable 8)** for all travel charged to the TO. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, Trip Reports shall be prepared with the information provided in the **Trip Report Template (Section J, Attachment G)**.



## SECTION C - PERFORMANCE WORK STATEMENT

### **C.5.1.8 SUBTASK 8 – PROVIDE QUALITY MANAGEMENT**

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a **Quality Management Plan (QMP) (Section F, Deliverable 9)** and maintain and update it as changes in the program processes are identified. The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements. The QMP is an evolutionary document that shall be updated periodically. At a minimum, the QMP shall be reviewed and updated annually.

### **C.5.1.9 SUBTASK 9 – DEVELOP AND MAINTAIN A TASK ORDER (TO) PORTAL**

The contractor shall develop and maintain an unclassified TO portal that Government-approved contractor personnel and Government personnel can access worldwide via unique user identification and password. The TO portal shall not be CAC enabled and shall be a cloud-based solution available to users with a .mil and a .gov account. Offerors shall provide a multi-factor authentication process with their TO Portal Strategy and identify this strategy in its proposal. The contractor shall provide the FEDSIM COR and the DTRA TPOC with the **TO Portal Strategy/Solution (Section F, Deliverable 10)** and a demonstration of the TO portal at the Program Kick-Off meeting. Once the FEDSIM COR has provided the contractor with the authority to proceed, the contractor shall proceed with developing and implementing the approved solution in a timely manner.

The objective of the TO portal is to introduce efficiencies and ensure coordinated service delivery. At a minimum, the TO portal shall serve as a repository for all unclassified TO deliverables and financial tracking data, including financial forecasts (**Section C.5.1.10**). The Government seeks innovation for managing workflow processes, and the portal shall include a workflow process that automates the submission of TO deliverables requiring Government approval such as, but not limited to, the submission of Rough Order of Magnitudes (ROMs), the contractor's Request to Initiate Purchase (RIP), Travel Authorization Requests (TAR), and Trip Reports. The workflow process shall allow the FEDSIM COR, DTRA TPOC, and other Government personnel (as required) to provide digital concurrence and approval of documents. The portal shall also be capable of Role-Based Access Control (RBAC) to limit access to the various workflows.

### **C.5.1.10 SUBTASK 10 – FINANCIAL FORECASTING**

The Government anticipates that DTRA's funding sources may vary (in terms of the color of money provided) and financial data will need to be tracked at the Military Interdepartmental Purchase Request (MIPR) level. The contractor shall work with the FEDSIM COR and the DTRA TPOC to determine the level of financial tracking required by the Government. The contractor shall create a financial forecast for each TO period of performance that details the anticipated monthly costs for labor, travel, and ODCs. The contractor shall set the baseline at the

## SECTION C - PERFORMANCE WORK STATEMENT

start of each TO period of performance and update the forecasts monthly, at a minimum, as costs are incurred or requirements change.

The contractor shall present a proposed format for the **Financial Forecast (Section F, Deliverable 11)** at the Program Kick-Off Meeting for FEDSIM COR and DTRA TPOC approval. Once approved, the contractor shall use the Government-approved format.

### **C.5.1.11 SUBTASK 11 – TRANSITION-IN**

The contractor shall provide a **Transition-In Plan (Section F, Deliverable 12)** as required in **Section F**. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. At a minimum, the Transition-In Plan shall identify all personnel positions to transition to the TO, when they transfer, and their role. The contractor shall implement its Transition-In Plan NLT the Project Start (PS) date and all transition activities shall be completed 90 calendar days after PS.

### **C.5.1.12 SUBTASK 12 – TRANSITION OUT**

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a **Transition-Out Plan (Section F, Deliverable 13)** within six months of PS. The contractor shall review and update the Transition-Out Plan in accordance with the specifications in **Sections E and F**.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- a. Project management processes.
- b. POCs.
- c. Location of technical and project management documentation, including Smart Book/Turnover binders containing copies of all plans, policies, and procedures.
  1. Transition of any data or documentation, to include information contained within the **TO Portal (Section C.5.1.9)** and the **Knowledge Management (KM) Database (Section C.5.5.7)**.
- d. Status of ongoing technical initiatives.
- e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel roles and responsibilities.
- g. Schedules and milestones.
- h. Actions required of the Government.
- i. Transition/return of any equipment provided by the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

## SECTION C - PERFORMANCE WORK STATEMENT

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO

### **C.5.2 TASK 2 – PLANNING, STRATEGY, AND ENGAGEMENT SUPPORT**

The contractor shall assess the current strategic planning efforts in order to verify that appropriate concepts, capabilities, technologies, and non-material solutions have been identified and incorporated to enhance the effectiveness of Counter WMD (CWMD) efforts and/or provide an understanding of threat networks. These assessments shall include the analysis of the integration plans and strategies and challenges within the Area of Responsibility (AOR)/Area of Interest (AOI). Additionally, the contractor shall conduct a **Planning and Strategy Gap Analysis (Section F, Deliverable 14)** in order to identify and mitigate potential risks present in DTRA or supported elements.

The contractor shall support the full range of analysis and planning activities at the strategic, operational, and tactical levels for DTRA. Planning is focused on the end state, globally integrated and coordinated, resource and risk informed, and framed within the Operational Environment (OE), and it is adaptable and flexible.

The contractor shall provide expertise to support the development of plans focused on areas that include, but are not limited to, Information Operations (IO); public affairs; Command, Control, Communications, and Computers (C4); and logistics to support the development, execution, management, and assessment of the family of military plans including theater and global campaign planning; U.S.-only planning; bi-lateral planning; country planning; Continuity of Operations (COOP); theater security plans; strategy and communications plans; and special program plans. This also includes **Contingency Plans, Operations Plans (OPLANs), and Operations Orders (OPORDs) (Section F, Deliverable 15)**. Generation of any of the plans listed herein shall be delivered in accordance with **Section F, Deliverable 15**.

The contractor shall be familiar with both deliberate and crisis action planning procedures and it shall be prepared to conduct truncated planning processes as required.

The contractor shall provide the following support to DTRA planning efforts:

- a. Draft and interpret high-level operational and organizational performance requirements.
- b. Support the development and monitoring of DTRA mission performance measures.
- c. Facilitate the development and review of tenant shared service agreements.
- d. Support the generation, writing, staffing, and coordination of doctrine and plans.
- e. Support the DTRA Technical Lead in ongoing revisions of **Operation Guides, Lessons Learned, Improvised-Threat Handbooks and Lexicons (Section F, Deliverable 16)**.
- f. Participate in DTRA supported DoD, interagency, and international development of WMD and **Improvised-Threat-Related Doctrine and Policy (Section F, Deliverable 17)**.
- g. Facilitate coordination of policy/documents.
- h. Review DTRA internal policy actions and strategic documents of interest and provide recommendations as appropriate based on guidance from the Government.

## SECTION C - PERFORMANCE WORK STATEMENT

- i. Support DTRA planning teams and/or participate in Government-directed emergency planning and any related exercises.
- j. Conduct mission analysis and planning for short-notice requirements and provide resulting recommendations to leadership.
- k. Monitor operations/tasks and respond to emergent Requests for Information (RFIs).
- l. Support strategic and operational engagements and prepare and coordinate **Staff Memoranda, General Officer/Flag Officer (GO/FO) Correspondence, and Briefings (Section F, Deliverable 18)**.
- m. Provide operational and technical expertise to support DTRA's Operational Effects (OPX) branch activities that support the full range of planning activities.
  - 1. Assist DTRA's OPX branch with development, integration, coordination, and synchronization of its plans and exercises to ensure they are aligned with OPX's mission.
  - 2. Review plans, doctrine, and OPX's requirements related to countering and deterring WMD, improvised threats, and threat networks at the strategic, operational, and tactical levels.
  - 3. Provide analytical, technical, and administrative support for day-to-day activities as it relates to the mission for the OPX.
  - 4. Support the development of OPX Mission-Essential Task Lists (METLs), standards, and conditions.
- n. Assist with planning and synchronization, reporting requirements, and updating records for all DTRA elements.

### **C.5.2.1 SUBTASK 1 – ENTERPRISE STRATEGIC ENGAGEMENT SUPPORT**

The contractor shall support DTRA's internal processes and procedures for engagement and communication with senior staff. This includes, but is not limited to, the following activities:

- a. Assist with the planning and execution of engagements and outreach programs.
- b. Draft and edit correspondence letters, **Policy Letters, Memoranda, Talking Points, and Notes** on behalf of the Government (**Section F, Deliverable 19**).
- c. Attend planning and engagement meetings and provide **Policy and Engagement Meeting Minutes (Section F, Deliverable 20)**.
- d. Maintain DTRA mission and Command briefings.
- e. Assist with staff and Command visits.
- f. Facilitate unclassified and classified meetings with industry, academia, and military experts to discuss innovations in CWMD, improvised threats, and threat networks.
- g. Provide logistical support and handle administrative details for meetings (i.e., duplication of materials, IT support, and IT technology to run on-site clearance and security checks).
  - 1. Coordinate with other agencies, organizations, or internal partners.
- h. Support approximately two to four meetings per month with up to four Subject Matter Experts (SMEs) in various fields of interest and up to four Strategic Interplay Exploration

## SECTION C - PERFORMANCE WORK STATEMENT

(SIE) events per year with up to ten SMEs. Topics for the meetings may range in classification level from non-classified to SECRET//No Foreign Nationals (NOFORN).

### **C.5.3 TASK 3 – OPERATIONAL EFFECTS (OPX)/SPECIAL ACCESS PROGRAMS (SAP) INTEGRATION**

SAPs assist the Combatant Commanders by providing technical/planning solutions in support of sensitive operational requirements for the DoD, CWMD, counter-improvised threat, and related Counter-Terrorism (CT) sensitive activities. This includes DTRA-funded SAPs, Alternative Compensatory Control Measures (ACCM) programs, Sensitive Technology Office (STO), and the DTRA Sensitive Integration Office (SIO). The analysis performed under this task assists Combatant Commanders with detection, deterrence, defeating, and illumination of networks, systems and associated TTPs designed, fielded, or employed unconventionally that are intended to adversely impact U.S. forces and coalition partners. This task requires integration

In support of this task the contractor shall:

- a. Provide sensitive activity support augmentation that enables emerging CCMD support requirements.
- b. Provide analysis on counter-improvised threat and CWMD operational effects to support Joint Task Force(s) and Technical Operations staff. Contractor staff may be required to embed with Government personnel to provide counter-improvised threat and CWMD operational effects support to Joint Task Force(s) (JTF) and Technical Operations staff.

#### **C.5.3.1 SUBTASK 1 – GENERAL TASK SUPPORT**

The contractor shall support research, analysis, integration, and sustainment of DTRA-funded SAP(s), ACCM programs, STO, and SIO initiatives for CCMDs and JTFs. This includes the establishment and operation of all SAP and STO facilities designated by DTRA.

The contractor shall:

- a. Provide expertise for Special Programs, STO, ACCM, and sensitive activity planning.
- b. Maintain situational awareness of SIO, special program, STO and sensitive activity plans, operations, and units, and provide an understanding of friendly/adversary capabilities in geographically designated CCMDs.
- c. Analyze Special Programs, STO, ACCM, Force Protection (FP), and sensitive activity capabilities for applicability and possible effectiveness in supporting current and future CCMD's efforts to CWMD, counter-improvised threat efforts, and provide reach-back support for these efforts to CCMDs and JTF(s).
- d. Provide **SAP, STO, ACCM, FP, and Capability Gap Analysis Reports (Section F, Deliverable 21)**.
- e. Use expertise and knowledge of SAP, STO, ACCM, and FP to provide analysis and capability Courses of Action (CoAs) that apply to countering WMD, and counter-improvised threats.

## SECTION C - PERFORMANCE WORK STATEMENT

- f. Assist in developing **SAP/STO Plans/Reports (Section F, Deliverable 22)** and provide the necessary training to provide continuity of operations for deploying Government personnel.
- g. Develop and prepare **SAP/STO Written Documents and Training Plans/memos (Section F, Deliverable 23)** (i.e., memos, information papers, significant activity, decision briefings, and briefing materials) to support DTRA in communications with DoD and Congressional leadership.

### **C.5.3.2 SUBTASK 2 – PROVIDE SAP SUPPORT FOR COMBATANT COMMANDERS**

The contractor shall provide expertise for the management of sensitive and classified programs and for existing and emerging SAP, STO, and sensitive activity initiatives that contribute to countering improvised threats and WMD challenges to include the coordinating and advocating the approval of SAP integration, and deployment to support Combatant Commanders. The contractor shall provide expertise to DTRA for SAP coordination, the SAP Information Security Program, the SAP Physical Security Program, the SAP Personnel Security Program, and other ACCM management activities at DTRA. Specifically, the contractor shall:

- a. Assist the Government with planning and coordinating functional security requirements for sensitive activities.
- b. Coordinate advanced and emerging SAP capabilities and technologies within current and future initiatives within DTRA.
- c. Support internal and external coordination, integration, de-confliction, and application of SAP activities/capabilities to support DTRA initiatives including, but not limited to, unit operation plans, contingency plans, and compartmented program plans.
- d. Provide SAP Facility Management (SAPFM) including process establishment, disestablishment, and restructuring of DTRA's SAPs.
- e. Provide coordination and integration for non-DTRA SAPs (where DTRA has been invited to participate).
- f. Provide expertise and support of efforts protected by ACCM in which DTRA participates as the originating activity or as a partner.
- g. Provide expertise to support Red Team and Wargaming activities as they pertain to SAP, including providing an independent capability to explore alternatives in plans, operations, concepts, organizations, and capabilities in the context of OE and from the perspective of partners and advisories.

### **C.5.3.3 SUBTASK 3 – CONUS/ OCONUS AND DEPLOYED SAP INTEGRATION SUPPORT**

The contractor shall provide sensitive activity integration directly to operations in OCONUS locations including, but not limited to, Europe, Asia, Africa, and South America. Integration efforts shall be accomplished using rotational personnel. The following table lists anticipated TDY locations for the first year of performance specific to SAP integration support.

## SECTION C - PERFORMANCE WORK STATEMENT

(Deployment/TDY locations may vary depending on the specific support required. Please refer to **Section F.2** and **Section J, Attachment J** for a complete list of performance locations.)

<b>CONUS Rotational Temporary Duty Durations by Location</b>	
<b>Location</b>	<b>Duration</b>
DTRA locations in Reston, Virginia (VA) and Tampa, Florida (FL)	No more than 45 days in duration
Headquartered in Fort Bragg, North Carolina (NC) and VA Beach, VA	No more than 45 days in duration
Headquartered in Crystal City, VA	No more than 45 days in duration
Headquartered in Stone Bay, NC	No more than 45 days in duration
Headquartered in San Diego, California (CA)	No more than 45 days in duration
Headquartered in Miami, FL	No more than 45 days in duration

In addition to the table above, personnel may be assigned to OCONUS locations in Hawaii and Germany. This assignment may include a permanent change of station (PCS) to Hawaii and Germany.

Contractor personnel may be required to support rotational Deployments/TDY's to other OCONUS locations. Deployments/TDYs are not anticipated to run longer than six months, excluding transit time. The TDY locations may cycle into austere or hazardous locations. Expected working hours during a rotational deployment/TDY are in accordance with **Section F.2.1**. The contractor shall:

- a. Participate in all aspects of operational planning, including mission analysis, course action development analysis, and operational concept development.
- b. Document operational planning activities and outcomes using traditional and emerging tools and formats associated with the Military Decision Making Process (MDMP) which includes, but is not limited to, mission analysis briefings; CoA decision and Concept of Operations (CONOPs) approval briefings; Decide, Detect, Deliver, Assess (D3A) execution matrices; generation of CONOPs documents; and generation of Fragmentary Orders (FRAGOs) (**Section F, Deliverable 15**).
- c. Integrate, synchronize, and facilitate compartmented, ACCM, and other technical capabilities, including available non-compartmented CWMD and counter-improvised threat capabilities and processes in support of the supported command's vision.
- d. Identify and facilitate planning, assessment, and operational integration of new or underused compartmented, ACCM, and other technical capabilities in support of CWMD and counter-improvised threat efforts.

## SECTION C - PERFORMANCE WORK STATEMENT

### **C.5.4 TASK 4 – PROVIDE LIAISON, INTEGRATION, AND WTI SUPPORT**

The contractor shall provide Integration and WTI support to Liaison Officers (LNOs) and Assistant Liaison Officers (ALNOs) to ensure synchronization of activities and capabilities across DTRA elements.

#### **C.5.4.1 SUBTASK 1 – PROVIDE LIAISON INTEGRATOR TEAM SUPPORT**

The Liaison Integrator team provides on-site integration and LNO support to CCMDs 24 hours a day, seven days a week (24x7) to ensure warfighters have instant access to a wide variety of DTRA capabilities. The Liaison Integrator team is responsible for coordinating DTRA personnel and activities within the CCMD AOR in order to enhance CWMD and threat network situational awareness and direct agency actions against threats. LNO, ALNO, and Integrator support is required at, but not limited to, the following locations:

- a. U.S. Central Command (USCENTCOM), MacDill Air Force Base (AFB), Tampa, FL.
- b. U.S. Indo-Pacific Command (USINDOPACOM), Camp H.M. Smith, HI.
- c. U.S. Special Operations Command (USSOCOM), MacDill AFB, Tampa, FL.
- d. U.S. Southern Command (USSOUTHCOM), Miami, FL.
- e. U.S. Transportation Command (USTRANSCOM), Scott AFB, O’Fallon Illinois.
- f. U.S. Forces Korea (USFK), Camp Yongsan Garrison, Republic of Korea (ROK).
- g. The Pentagon, Washington, D.C.

These locations are specific to LNO Integrator Team and Assistant LNO (ALNO) support. Contractor personnel assigned to USFK, USSOCOM, USCENTCOM, USSOUTHCOM are considered deployable. For additional performance locations please see **Section J, Attachment J** and **Section F.2**.

#### **C.5.4.2 SUBTASK 2 – PROVIDE LIAISON INTEGRATOR AND ASSISTANT LNO (ALNO) SUPPORT**

The contractor shall provide LNO and ALNO support at regional and functional commands and the Pentagon. This support requires a minimum of four ALNO positions to be designated as “deployable.” This designation means the individual occupying one of the deployable ALNO positions must annually meet the specific deployment training as described in **Section H.8**. The contractor shall:

- a. Provide on-site support to DTRA including, but not limited to, providing LNO or ALNO support to senior leadership in developing the evolving agency vision, goals, and objectives. This includes coordination with DTRA and other stakeholders.
- b. Provide analytical and technical support to LNO/ALNO team training. This includes **LNO/ALNO Course Preparation (Section F, Deliverable 24)**, development of **LNO/ALNO Training Plans/Records (Section F, Deliverable 25)**, and preparation of historical files.
- c. Prepare, develop, and create scenarios for LNO/ALNO team (**Scenario Development (Section F, Deliverable 26)**).



## SECTION C - PERFORMANCE WORK STATEMENT

- d. Provide analytical and technical support for day-to-day surge activities including routine reporting requirements and updating administrative rosters and records. Provide support to short notice tasks.
- e. Support the LNO/ALNO team during exercises and contingencies.
- f. Assist the DTRA with development, coordination, and integration of DTRA **plans, policies, and procedures** in support of the CCMDs (**Section F, Deliverable 15**).
- g. Provide continuity of support that facilitates instruction and training of newly assigned members of the LNO/ALNO team and provides reach-back.
- h. Develop and prepare **LNO/ALNO Briefing Materials, Papers, and Analysis** (**Section F, Deliverable 27**).
- i. Prepare and present technical and operational reports. Assist with identifying and resolving key issues and preparing briefing materials on program plans, requirements, and progress.
- j. Assist with the organization, coordination, and support of workshops; coordinate review meetings; and support DTRA LNOs with attendance, documentation, and follow-up of meetings, conferences, and exercises relevant to DTRA's mission.
- k. Coordinate and track visits to CCMD headquarters or AOR by key DTRA personnel.
- l. Monitor feedback regarding DTRA programs including, but not limited to, maintaining situational awareness of CCMD key activities, personnel, and issues of interest to DTRA leadership; assisting with review and coordination of CCMD OPLANs, Contingency Plans (CONPLANs), and Functional Plans (FUNCPLANs); and supporting agency analyses and plan development.
- m. Assist in identifying emerging technologies that are relevant to the CCMD's and DTRA's mission and support the coordination of planning and operations through DTRA's Joint Operations Command (JOC) by maintaining continual communications with that entity.

### **C.5.4.3 SUBTASK 3 – PROVIDE COMBAT INTEGRATION SERVICES**

DTRA has a formal RFS process that reflects a methodology for the timely delivery of analytical requirements of DTRA internal customers. A key ingredient of the RFS process is delivery of the requested support within the timeframe identified on the RFS. The contractor shall respond to the RFS in accordance with the template provided, **RFS Template (Attachment H, Section J)**. Any reports or analyses produced from the RFS process shall be delivered to the Government as **RFS Reports (Section F, Deliverable 28)**. The contractor shall develop teams of individuals with a variety and mix of expertise required to address the RFS requirements and collaborate with DTRA to conduct the analysis of counter-threat network operations.

Specifically, the contractor shall:

- a. Receive RFSs and coordinate assignment of the requirement for action to the appropriate analytical support team(s).
- b. Maintain visibility of all RFSs and required actions identified through the **RFS Tracker (Section F, Deliverable 29)** and track RFS through to completion and close out.
- c. Maintain and retain copies of RFS reports delivered.

## SECTION C - PERFORMANCE WORK STATEMENT

- d. Support Government quality assurance reviews as the response to the RFS is developed.
- e. Provide an on-site interface to all CCMDs and field activities through a 24x7 watch.
  - 1. Maintain the 24x7 watch and ensure it is manned with analysts that can communicate with other commands/agencies.
  - 2. Produce **Daily/Weekly/Monthly Global Slides** and the **Director's Update (Section F, Deliverable 30)**.
- f. Provide assessments of overall RFS activities and trends.
- g. Deliver and coordinate **Combat Support Technical Reports (Section F., Deliverable 31)**.
- h. Inform Coalition partners of Five Eyes (FVEY) releasable reports and provide access as requested.
- i. Provide daily qualitative and quantitative analysis of RFS and analytical efforts.
- j. Develop trained Data Transfer Officers (DTOs) for transfers of information across networks of multiple levels of security (Low to High and High to Low).
- k. Deliver and coordinate **Global Improvised Threat Reports (Section F, Deliverable 32)**, as required.

### **C.5.4.4 SUBTASK 4 – PROVIDE OPERATIONS INTEGRATION**

The contractor shall provide operations integration and analytical support on counter-improvised threats and CWMD analysis that is used to inform field commanders up through CCMD staff on the capabilities and tools available through DTRA. The contractor shall provide operational, analytical, and training reach-back assistance through DTRA's RFS process. Personnel working on this task may deploy and provide the stated services in HD/CZ. The FEDSIM COR in coordination with the DTRA TPOC may waive or postpone deployment specific training, identified in **Section H.8**, on an individual or group basis. Specifically, the contractor shall:

- a. Provide operational experts that are embedded with Government personnel at the CCMD to facilitate analysis and integration of information provided by DTRA.
- b. Ensure that **RFS Reports (Section F, Deliverable 28)** meet the operational objectives of the command supported.
- c. Provide specialized expertise in military operations for interaction directly between unit Commanders, DTRA support elements, and personnel during the development of analysis reports, in order to fuse operational information with the information available, and provide an operational perspective throughout the planning cycle.
- d. Support the Government's efforts to identify kinetic and non-kinetic measures that military and non-military Government authorities can take to mitigate, frustrate, or thwart threat network operations, directly or indirectly, based on available conventional and unconventional analysis.
- e. Support the Government's analysis and the development of tactical, operational, and strategic initiatives that codify successful approaches to interdicting the value chain to frustrate and neutralize improvised and WMD devices and operations, including component trans-shipment.

**C.5.4.5 SUBTASK 5 – PROVIDE WTI ANALYTICAL SUPPORT**

The contractor shall provide WTI research and analysis support for WMD and improvised CBRNE, explosives, devices, and their uses; trend and pattern analysis; geospatial analysis; link analysis; and network or social network analysis. The contractor shall use computer applications to automate analytical efforts and product development. To support WTI analysis, the contractor shall use its expertise in analysis-related IT systems (i.e., Distributed Common Ground System-Army (DCGS-A), Combined Information Data Network Exchange (CIDNE), Secret Internet Protocol Router Network (SIPERNET)/Joint Worldwide Intelligence Communications Systems (JWICS) search engines); and, it shall use its experience with i2 Analyst Notebook, AXIS Pro, Web-enabled Timeline Analysis System (WebTAS), Weapons Technical Analysis Exploitation Analysis Tool (WEAT), ExPERT, ArcGIS and Google Earth to facilitate analysis. Specifically, the contractor shall:

- a. Support Government efforts to identify and research new devices, initiators, and TTPs on which to focus analytic efforts.
- b. Conduct technical research and analysis of WMD and improvised weapons, fusing the information with other forensic data and all-source data to provide attribution of individuals and groups to devices and events.
- c. Analyze devices and events to determine WMD profiles and patterns.
- d. Identify insurgent threat networks, including leaders, facilitators, financiers, cell members, and bomb makers, to identify potential targets for possible lethal and non-lethal action.
- e. Develop and prepare **WTI reports/analyses (Section F, Deliverable 33)** that include, but are not limited to, regional device pattern and trend studies, route device pattern and trend studies, TTPs, vulnerabilities and countermeasures studies, and WMD and improvised threat technical profiles.
- f. Support planning, policy generation, and engagement as it relates to WTI in accordance with **Section C.5.2**.
- g. Develop, prepare, and present **WTI Briefings/Reports (Section F, Deliverable 33)**; evaluate information reporting and sources; answer analysis related RFIs; and develop source directed requirements.
- h. Develop and prepare WTI-related assessments for formal production and release to the Intelligence Community (IC) and other consumers, and coordinate with other Government offices, IC, and law enforcement, including the Federal Bureau of Investigation's (FBI) Terrorist Explosives Device Analytical Center (TEDAC) and Theater resources, to gather additional technical and forensic data and share analytic conclusions.
- i. Support DTRA's efforts to assist Coalition and International Partners with analyzing data obtained from the exploitation of materials in accordance with applicable standards, policies, and regulations.

## SECTION C - PERFORMANCE WORK STATEMENT

- j. Identify data and information requirements and identify/assess gaps in existing exploitation databases and IT architecture to support improvements and capability development.
  - 1. Support data curation and KM efforts in accordance with **Sections C.5.5.6 and C.5.5.7**.
    - i. Develop reports and briefings and make recommendations to explain the essential elements of WTI capabilities (**Section F, Deliverable 33, WTI Reports/Briefings**).
    - ii. Support interagency working groups where WTI capabilities, data management, and knowledge sharing are discussed.
  - 2. Support implementation and improvement of WTI strategies, management practices, internal controls, and efforts to improve operational effectiveness.
- k. Provide analytical support to deployed and reach-back exploitation laboratories.
- l. Conduct logistics and material acquisition related to WTI in accordance with **Sections C.5.9.6 and C.5.9.7**.

### **C.5.4.5.1 SUBTASK 5.1 – PROVIDE LAW ENFORCEMENT TECHNIQUES AND DETAINEE INFORMATION EXPLOITATION**

The contractor shall tailor and apply law enforcement techniques and insights to develop case files on individual threat actors that are identified by deployed law enforcement specialists in theater. Specifically, the contractor shall:

- a. Provide expertise in law enforcement techniques to integrate law enforcement information with WMD and improvised threat analysis.
- b. Develop threat network diagrams, case files, and conduct biometric analysis regarding the criminal behavior of individuals based on the information provided by deployed law enforcement specialists.
- c. Coordinate with other analytical teams to integrate law enforcement information, including investigative material developed in theater, into broader analytical efforts.
- d. Provide reach-back capabilities to harness information in the law enforcement communities (Federal and appropriate Defense Agencies).
- e. Identify emerging criminal trends and methods of operation in order to deter and interdict networks associated with the sourcing, production, delivery, and emplacement of WMD and improvised threats.
- f. Compile, build, and manage detainee-related information for exploitation during detainee interrogations in support of RFS from theater.
- g. Deliver technical reports that respond to RFSs (**Section F, Deliverable 28, RFS Reports**).

### **C.5.4.5.2 SUBTASK 5.2 – PROVIDE COLLECTED EXPLOITABLE MATERIAL (CEM) PROGRAM ANALYSIS AND FORENSIC SCIENTIFIC SUPPORT**

The contractor shall provide CEM program analysis to that supports the collection, exploitation,

## SECTION C - PERFORMANCE WORK STATEMENT

and analysis of WMD, improvised weapons/threats, and associated components. The contractor shall provide program analysis and management of related forensic, biometric, and scientific programs. The contractor shall provide analysis and management of related technical exploitation projects and programs to include electronic, mechanical, media, and document exploitation.

Additionally, the contractor shall:

- a. Maintain current knowledge of and leverage CEM capabilities across DoD, academia, interagency, international stakeholders; and work closely with Government scientists, engineers, national laboratories, and allied organizations to coordinate, advocate, and develop CEM capabilities in support of DTRA and CCMD goals and objectives.
- b. Support DTRA's efforts to develop and integrate existing DoD CEM and emerging Forensic and related science and technology requirements, policies, and capabilities that pertain to the sharing of CEM.
  1. Ensure the resulting information and data management supports exploitation outcomes and DoD programs, including forensics, biometrics, technical exploitation, and sensitive site exploitation programs.
  2. Ensure data tagging and curation in accordance with **Sections C.5.5.6 and C.5.5.7**
- c. Monitor forensics and scientific related research, development, test, and evaluation communities to identify and assess trends and developments in forensic modalities and other related efforts, including human signatures, source attribution, and trace chemistry.
- d. Support DTRA with the integration of traditional and expeditionary forensic capabilities across all scientific disciplines.
- e. Provide guidance to DTRA's supported CCMDs to ensure forensic capabilities are used to their fullest capability/capacity in support of CWMD and counter-improvised threat operations.
- f. Support DTRA's efforts to develop and synchronize forensic scientific standards, processes, procedures, best practices, and lessons learned across expeditionary and reach-back laboratories.
  1. Maintain a common understanding of current forensic and biometric training efforts across the DoD and make recommendations to improve these programs to meet operational requirements.
  2. Support efforts to assess, develop, and synchronize DTRA's requirements and capabilities that pertain to technical exploitation of recovered materials.
- g. Support Government efforts to determine the suitability and feasibility of science and technology proposals and research projects taking into consideration factors such as the technical competence of the people involved, relevancy and effectiveness of the work proposed, alternative solutions available, cost, schedule, and performance.
- h. Support the Government with development of project agreements with coalition and host nations by providing assessments of capabilities and policies.
- i. Support DTRA's efforts for strategic communication, outreach, working groups, and other meetings with external stakeholders and partners regarding CEM information.

## SECTION C - PERFORMANCE WORK STATEMENT

1. Prepare and provide reports and briefings (**Section F, Deliverable 34, WMD/CEM Briefings, Reports, Analysis**), and make recommendations to explain the essential elements of forensic and scientific capabilities.
2. Support the implementation of new or improved forensics and biometric strategies, management practices, and DTRA internal controls to improve operational effectiveness and integrate capabilities.
- j. Maintain an awareness of current scientific developments within the national and international forensic science and technical communities. Apply professional knowledge in biological science, Deoxyribonucleic Acid (DNA) analysis, and quality assurance/quality control relating to DNA and serological analysis of evidence.
- k. Research and provide professional analysis of forensic systems currently fielded within DTRA to determine the technical capabilities and deficiencies. Based on operational requirements and expert analysis, develop a detailed analysis of **Technical Capability Gaps (Section F, Deliverable 35)**. Work with DTRA, to understand needs and address capability gaps.
- l. Support the implementation of new or improved CEM strategies, management practices, and DTRA internal controls to improve operational effectiveness and integrate capabilities.

### **C.5.4. 5.3 SUBTASK 5.3 – PROVIDE THEATER OPERATIONS SUPPORT**

The contractor shall support the operational assessment, implementation, and execution of collection, exploitation, and analysis capabilities that pertain to counter-improvised threat and WTI capabilities that are deployed in support of CCMD operations. The contractor shall provide expertise in the areas of WMD and improvised threat exploitation, including forensics, biometrics, technical exploitation, and site exploitation. Additionally, the contractor shall:

- a. Support expeditionary exploitation requirements in support of CCMD requests.
- b. Support DTRA, CCMD and coalition training and exercises to ensure proper integration of exploitation capabilities.
- c. Assist in the identification and development of **CEM/WTI Training and Exercise Plans (Section F, Deliverable 36)** and **CEM/WTI Lessons Learned (Section F, Deliverable 37)**.
- d. Assist tracking and assessing existing collection and exploitation capabilities and support of DTRA's efforts to identify new capabilities.
- e. Maintain current awareness of evolving threats and coordination of efforts across CCMDs and international partners that pertain to collection and exploitation support requirements.

### **C.5.5 TASK 5 – ANALYTICAL SUPPORT**

DTRA provides direct analytical support to CCMDs and their deployed forces. This specific analytical support will enable cohesive response to counter threat networks and provides steady-state support for DTRA missions and deployable expertise with reach-back capability. In support

## SECTION C - PERFORMANCE WORK STATEMENT

of this task, the contractor shall perform strategic all-source analysis in the areas specified by the subtasks below.

As part of this task, analytical support may be required in deployed environments, and the individuals assigned would be subject to the required training identified in **Section H.8**. The FEDSIM COR in coordination with the DTRA TPOC may waive or postpone deployment-related training on an individual or group basis.

The contractor shall:

- a. Produce analytical assessments and reports.
- b. Provide indications and warnings.
- c. Identify CWMD threat and capability gaps and provide potential CoAs.
- d. Integrate existing national-level reports/analyses and databases to provide an enhanced level of information support.
- e. Conduct multi-layered research and analysis in cooperation to define and assess patterns of human and enemy network activities for support of counter-improvised threat and CWMD operations.
- f. Provide expert support countering threat networks that use improvised threats and WMD. Expert support shall use qualitative and quantitative research and analysis, training, and technology. The contractor shall employ advanced tools for information collection and analysis to enhance the ability of deployed Government forces to eliminate or neutralize enemy insurgent networks that threaten U.S. interests and employ improvised threats and/or WMD.
- g. Support the Government's research and development of tactical, operational, and strategic initiatives that codify successful approaches to interdicting the value chain to frustrate and neutralize improvised and WMD devices and operations, including component trans-shipment.
- h. Maintain a global knowledge base of current and future improvised and WMD threats to provide solutions to counter vulnerabilities.
- i. Develop analyst-to-analyst communications with operational and tactical consumers of information to incorporate all analytic strengths presented by participating agencies, organizational activities, and available technology into the analysis.
- j. Provide specialized expertise in military operations for interaction directly between DTRA and unit Commanders. Support DTRA by fusing operational information and analysis available to provide an operational perspective throughout the operational planning cycle.

### **C.5.5.1 SUBTASK 1 – ALL-SOURCE ANALYTICAL SUPPORT**

The contractor shall provide all-source analysis to enable CWMD, counter proliferation, counter-improvised threats, build partner capacity, and nuclear surety and response. The all-source analysis fuses inputs from all levels and multiple disciplines to produce assessments meant to reduce strategic surprise and inform policy/DoD decision makers. The contractor shall provide

## SECTION C - PERFORMANCE WORK STATEMENT

innovative research, data, tools, and analysis to better understand threat value chain and associated personalities, nodes, relationships, and activities comprising and characterizing improvised threats, WMD threats, and associated threat networks. The all-source analysts shall specialize in network analysis and the following:

- a. Technical Analysis (TECHINT).
- b. WMD analysis.
- c. Targeting analysis.
- d. Find, Fix, Finish, Exploitation, Analysis, and Dissemination (F3EAD).
- e. Threat finance analysis.
- f. Human Information (HUMINT).
- g. Geospatial Information (GEOINT).
- h. Open Source Analysis (OSINT).
- i. Irregular Warfare Analysis (IWA).
- j. Signals Information (SIGINT).
- k. Document and Media Exploitation (DOMEX).
- l. Measurement and Signals Information (MASINT).
- m. Operations and Research Systems Analysis (ORSA).
- n. Crime pattern analysis.
- o. Law enforcement operations analysis.
- p. Detainee exploitations analysis.

The contractor shall organize and conduct multi-layered assessments by researching, evaluating, and integrating all-source data in the production of all-source assessments. The contractor shall use the information gained from multiple and varied sources to produce **All-Source Operational and/or Strategic-Level Assessments (Section F, Deliverable 38) and All-Source Reports and Fusion Products (Section F, Deliverable 39)** that address countering threat networks that use improvised threats or WMD. These assessments shall conform to organizational, community, oversight, and regulatory requirements. These assessments will enable the generation of operational effects options for DTRA to develop, shape, and execute effects-based counter threat network operations.

Specifically, the contractor shall:

- a. Assess facts, threat intents, and cultural behavioral norms.
- b. Assess the implications of the environment to determine if there is friendly and adversarial involvement in that environment.
- c. Predict an accurate indication of adversarial intent, capabilities, vulnerabilities, and potential threat CoAs.
- d. Provide a deep understanding of insurgencies, irregular warfare, Violent Extremist Organizations (VEO), and state actors.



## SECTION C - PERFORMANCE WORK STATEMENT

- e. Collect management, targeting, imagery, network research and analysis, moving target indications, backtracking, counterintelligence, CT, foreign disclosure, international engagements, and threat research and analysis.
- f. Provide exploitation and asymmetric threat research and analysis that include the identification and integration of countermeasure technologies and the potential optimized employment of Intelligence, Surveillance, and Reconnaissance (ISR) assets to support counter-improvised threat and CWMD operations.
- g. Conduct research and analysis of Explosive Ordinance Device(s) (EOD)/weapons reporting from exploited improvised threat materials/devices in order to link them to other materials/devices of similar origin or construction.
  - 1. Combine assessments with HUMINT, SIGINT, biometric research and analysis, and other analysis disciplines for the purpose of attribution.
- h. Conduct counter-improvised threat and CWMD research to identify issues and provide alternatives for issue resolution. Employ traditional analysis techniques (e.g., HUMINT, MASINT, Imagery Analysis (IMINT), and OSINT) and forensic accounting to provide information that will interrupt and destroy threat cells and networks along with any Command and Control (C2) capabilities. Forensic accounting analysis may include tracing financial interactions and tracking instances of bribery, reverse money laundering, business information, or theft ring targeting.
- i. Conduct open source unconventional discovery, research, fusion, and analysis using nontraditional methods to search, find, acquire, normalize, and integrate open source data using best-of-breed applications; cutting-edge tools; and emerging techniques, methodologies, and procedures to integrate unconventional information with mainstream-fused, all-source analytic efforts.
- j. Determine “fact of” relationships, establish normal activity baselines, and uncover masked or hidden relationships (e.g., network-to-network relationships and nation state involvement). Conduct analyses regarding personality, node and activity trends, patterns, and deviations.
- k. Access, harness, and leverage bulk data, big data, and social media to inform and drive the all-source counter-improvised threat and WMD analytic process.
- l. Integrate data originating from a wide variety of incongruous sources in disparate and incompatible formats, including conversion of defined and digestible data sets to common ontologies for potential ingestion and use for Government purposes.
- m. Exploit resolved data for data layering and fused research and analysis. Conduct recursive data mining to expose multiple layers of identified information, from disambiguation to biometrics, and all aspects of digital identity, including virtual and real.
- n. Illuminate, identify, and conduct detailed deconstruction of personalities, entities, producers, distributors, retailers, regulators, and enablers that comprise the global improvised threat and WMD component value chain, as well as the financial and facilitation networks that work in support of threat networks involved in improvised threat device and WMD operations and other nefarious activities.

## SECTION C - PERFORMANCE WORK STATEMENT

- o. Detect, map, and analyze the corporate entities; regulatory bodies; trans-shipment points; enabler networks; and personnel, material, and financial flows that comprise the global improvised threat and WMD component value chain.
- p. Provide analysis to DTRA decision makers that identifies kinetic and non-kinetic measures Government authorities can take to mitigate, frustrate, or thwart threat network operations, directly or indirectly, based on available information and analysis.

### **C.5.5.2 SUBTASK 2 – IRREGULAR WARFARE ANALYSIS (IWA)**

IWA is a specialized analytical activity that employs advanced analysis of TTPs and expert understanding of insurgent-based unconventional warfare to conduct associative targeting of individuals, cells, network C2, and logistics in support of CCMDs. IWA employs critical, relevant, and effectual pattern analysis on insurgent-based operations in mapping out cells and networks to fight the Global War on Terrorism (GWOT). This involves a select application of collective analysis techniques and methodologies combined with U.S. Special Forces-centric in-depth understanding of insurgent-based unconventional and irregular warfare. Irregular warfare and Fusion Analysis Deployment Effort (FADE) Analysts are integrated with other disciplines, as needed, and support the production of **IWA Analysis Products (Section F, Deliverable 40)**.

The contractor shall provide the following IWA services including, but not limited to:

- a. Engage in a systematic identification, research, and analysis of cells and networks germane or associated with the financing, construction, and employment of improvised weapons and WMD, as well as the purveyors of such material.
- b. Focus on data that informs DTRA of the existence, organization, and operation of threat networks, including data that provides insight into technical, tactical, operational, and strategic capabilities. Specific data analysis required includes the following:
  - 1. Information on threat network structures including the identification of individuals and relationships between various individuals and groups, organizational constructs, and other relevant data. This includes names, nicknames, locations, affiliations, technical proficiency, levels of training, and positions within a network or community.
  - 2. Information on threat operational capabilities including TTPs, cover and deception methods, targeting strategies, and surveillance methods.
  - 3. Information on threat technologies including raw materials, manufacturing processes, supply chains, usage intentions, and any identified operational opportunities for the U.S. Government.
  - 4. Pattern of Life study inputs that may lead to knowledge of the whereabouts of individuals of interest or concern.
- c. Provide predictive analysis on specific likely evolutions in adversary TTPs and operations.
- d. Develop notional concepts of operations and CoAs that best represent likely adversary activity.
- e. Assist DTRA with the integration of analysis.

## SECTION C - PERFORMANCE WORK STATEMENT

- f. Assist DTRA with providing responses to information requests, questions, or concerns regarding reports or strategic assessments.

### **C.5.5.3 SUBTASK 3 – TARGETING ANALYSIS**

Targeting analysis requires the contractor to understand, comply with, and possess an in-depth knowledge of Joint Staff and theater targeting guidance, Battle Damage Assessments (BDA) guidance, and collateral damage guidance. The contractor shall provide Target System Analysis (TSA) of threat platforms and organizations that support operational planning and targeting efforts. The contractor shall conduct research of all-source reporting to produce finished information **Targeting Analysis Reports/ Packages (Section F, Deliverable 41)**.

The contractor shall provide expert targeting analysis services against High Value Individuals (HVI). The contractor shall use information, qualitative and quantitative research and analysis, training, and technology and employ tools for information collection to enhance an RFS customer's F3EAD targeting cycle in support of counter-VEO operations.

In support of this task, the contractor shall provide analysts with the capability to embed with Government personnel in fast-paced, high-priority, military operations centers that may be deployed anywhere in the world to support counter-VEO analysis. Contractor personnel assigned to this task shall have expert knowledge of high priority VEO threat networks, leadership structures of the threat networks and personalities, and TTPs and vulnerabilities of those networks. Contractor personnel shall be able to pass a special assessment that includes a physical examination, psychological examination, and a suitability assessment conducted by the supported DTRA unit.

Specifically, the contractor shall:

- a. Provide individuals that are suitable for access to ACCM information, material, and systems.
- b. Provide expertise in the employment and control of ISR assets in support of targeting operations.
- c. Provide expertise in the exploitation of operations and CEM that supports the F3EAD targeting cycle.
- d. Provide expertise in detainee operations including identifying information support to interrogations that support the F3EAD targeting cycle.
- e. Provide expertise in HUMINT operations that support the F3EAD targeting cycle.
- f. Provide expertise in SIGINT analysis and SIGINT tools and methodologies that support the F3EAD targeting cycle.
- g. Provide expertise in OSINT that support the F3EAD targeting cycle.
- h. Provide expertise in GEOINT that support the F3EAD targeting cycle.
- i. Provide targeting analysis and produce **Target Analysis Packages (Section F, Deliverable 41)** targeting vignettes and written assessments of associated targets, especially profiles of network individuals and entities and their activities, in order to enable kinetic, unilateral force and partner force operations.

## SECTION C - PERFORMANCE WORK STATEMENT

### **C.5.5.4 SUBTASK 4 – CURRENT ANALYSIS**

DTRA requires timely, vetted analysis that provide insight into countering or defeating WMDs and improvised threats. Operational analysis from multiple sources must be provided within the timeline requested in the RFS. Such analysis will be used by deployed military tactical forces to conduct offensive operations against insurgent threat networks.

To support this effort, the contractor shall provide **Current Analysis Reports** to DTRA (**Section F, Deliverable 42**). Specifically, the contractor shall:

- a. Monitor and report priority requirements and issues relevant to DTRA's Director and respond to RFS(s) (**Section F, Deliverable 28**) from DTRA.
- b. Prepare and deliver the **Daily/Weekly Update (Section F, Deliverable 30)** for DTRA's Director.
- c. Provide information and analysis support to DTRA working groups and analytical teams.
- d. Conduct continuous research and maintain an awareness of current WMD and improvised threat technology and TTPs used by the state and non-state human enemy networks.
- e. Apply all-source analysis to improve the effectiveness of WMD and improvised threat to global situational awareness operations.
- f. Deliver and coordinate **Current Analysis/Improvised-Threat Reports (Section F, Deliverable 42)**.
- g. Prepare and deliver the **Priority Intelligence Requirements (PIR) Documents (Section F, Deliverable 43)**.

### **C.5.5.5 SUBTASK 5 – ANALYSIS AND ASSESSMENT SUPPORT**

The contractor shall conduct analysis, as directed by the Government, in order to identify threats, identify risks, and recommend how DTRA and CCMDs can best defend themselves. As global challenges arise and evolve, the contractor shall continually assess the environment using a variety of methods (e.g., media monitoring), and it shall provide the Government with the **Analysis and Assessment Reports (Section F, Deliverable 44)** focused on topics that include, but are not limited to:

- a. Non-traditional information collection activities.
- b. Threat trends.
- c. Current and/or emerging crises.
- d. OEs (including, but not limited to, the political, military, economic, social, information, infrastructure, and physical environment of the area).
- e. Terrorism/counter terrorism.
- f. Anti-terrorism (AT) and FP threats.

At a minimum, assessment reports shall detail the research conducted, the analysis performed, risks and potential impacts, and any recommendations for the Government to consider. The

## SECTION C - PERFORMANCE WORK STATEMENT

contractor shall also support the development and implementation of potential outputs from the assessment reports by providing analytical and technical expertise to assist the Government.

### **C.5.5.6 SUBTASK 6 – PROVIDE COLLECTION REQUIREMENTS SUPPORT**

The contractor shall provide support to improve the reporting available to DTRA from the IC by standardizing and communicating collection requirements to the appropriate agencies. The contractor shall:

- a. Assist with the validation, coordination, submission, and maintenance of formal analysis requirements and requests to the DoD/IC.
- b. Assist DTRA with understanding shared analysis that is collected by DTRA and/or other Government and DoD partners. This includes assisting DTRA with understanding how the analysis collected can be utilized to inform DTRA leadership.
- c. Ensure DTRA's collection requirements are incorporated into national and theater level collection requirements management process.
- d. Ensure DTRA's collection requirements are integrated with analysis activities and reports.
- e. Apply its experience with IC collection management systems and mission applications to ensure complete and clear understanding of collection information (i.e., Collection Requirement Analysis Tool for the Enterprise (CRATE), Planning Tool for Resource Integration, Synchronization, and Management (PRISM), Community Online System for End-Users and Managers (COLISEUM), Geospatial Intelligence Management System (GIMS), National SIGINT Requirements Process (NSRP), National MASINT Requirements System (NMRS), HUMINT Online Tasking and Reporting (HOTR), and Open Source Collection Acquisition Requirement-Management System (OSCAR-MS).
- f. Deliver technical analysis that respond to RFS Reports (**Section F, Deliverable 28**).

### **C.5.5.7 SUBTASK 7 – PROVIDE REPOSITORY CURATION/ DATABASE KNOWLEDGE MANAGEMENT (KM)**

Unclassified (open source) and classified CWMD and counter-improvised threat data are integrated in authoritative analytical databases. DTRA requires KM to enable on-demand, user-friendly RBAC access to vetted, collected, and correlated data.

The contractor shall provide KM support with the objective of fostering information sharing and enhanced decision making. The contractor shall capture analysis through proper data tagging and develop a **KM Plan (Section F, Deliverable 45)**. The KM strategy should utilize industry best practices and procedures, be tailored to the current requirements, and be adaptable to incorporate future requirements. The contractor shall create a **KM Data Repository (Section F, Deliverable 46)**. All data captured, managed, and stored shall transition to the Government at the end of the period of performance of this TO.

In order to populate the KM Data Repository, the contractor shall research topics that address gaps within Government-directed repository databases using classified and unclassified military databases to incorporate appropriate analysis products into the KM Data Repository. The

## SECTION C - PERFORMANCE WORK STATEMENT

contractor shall utilize Open Source research techniques, foreign languages, explosive ordinance disposal techniques, WTI analysis, advanced social network analysis, and cultural expertise to conduct large scale media analysis (including foreign language media) combined with in-depth research to populate the KM Data Repository.

The contractor shall create and provide a **KM Data Repository SOP (Section F, Deliverable 47)** that is consistent with Government-approved analytical repository SOPs and generate the associated **KM Data Repository Training Materials (Section F, Deliverable 48)**. The contractor shall use Government-approved domains to develop, build, manage, and maintain collaborative environments at both the unclassified and classified levels (SIPRNET). In developing and maintaining these environments, the contractor shall comply with DTRA and DoD standards.

The contractor's KM services shall:

- a. Enable the ability to store, link, extract, and clean organizational data records within Government analytical repository databases.
- b. Conduct data conditioning and storage of organizational data while maintaining traceability to its original sources.
- c. Curate user- or machine-provided data within organizational databases, ensuring record cleanliness, accuracy, and integrity of data.
- d. Initiate, coordinate, conduct, and/or curate research products to populate the KM Data Repository.
- e. Provide the ability to produce periodic **KM Metric Reports (Section F, Deliverable 49)** on the KM database metrics and trends.
- f. Support the development of metadata standards and protocols and review information repositories associated with exploitation data networks and databases.

### **C.5.6 TASK 6 – SPECIALIZED ANALYSIS**

Expert functional and specialized analysis enables the Government to develop and implement strategies, plans, policies, and actions to counter and deter WMD, improvised threats, and threat networks. In order to be successful at its mission, DTRA acquires and maintains an in-depth working knowledge and tactical understanding of the enemies' perspective of human networks that use or facilitate the use of WMD and improvised threats. To support countering WMD and improvised strategy development, DTRA requires war-gaming/red-teaming to enhance CWMD and counter threat strategy development. Additionally, specialized analytical support provides deep expertise beyond the training and capability of all-source analysts and will augment deployed and reach-back teams with specific information not otherwise available. The contractor shall provide specialized analytical expertise in the following areas: GEOINT, IMINT, MASINT, OSINT, threat finance analysis, open-source analysis, critical factors analysis, and law enforcement techniques and detainee information exploitation.

**C.5.6.1 SUBTASK 1 – EXERCISE SUPPORT (RED-TEAMING/WAR-GAMING)**

The contractor shall provide exercise support that includes a Red Team capability focused on providing tactical, strategic, and technical threat scenarios. **Tactical Red Teams** provide CWMD and counter-improvised threat scenarios that can support tactical forces, battle-space owners, and Forward Operating Base (FOB) security. **Strategic Red Teams** provide geographic-centric threat scenarios to Combatant Commanders that support CCMD operations, decisions, and resource allocations. **Technical Red Teams** provide threat TTPs and technological advancements/changes to CWMD and counter-improvised threats.

The contractor shall utilize expertise in irregular/asymmetric warfare enemy techniques including unconventional warfare, CT, and tactics and ensure cultural analysis including anthropological, political, religious, economic, and social issues are included in any **Red Team/War-Game Scenarios/Reports (Section F, Deliverable 50)**. In support of Red Teams, the contractor shall:

- a. Provide possible enemy CoAs for the employment of WMD and improvised threats
- b. Remain prepared to support war-gaming and SIE system production efforts with detailed enemy CoAs and Red Role Players.
- c. Provide open-source research and analytical support for scenario development that identifies and assesses trends that impact efforts to counter and deter WMD, improvised threats, and threat networks.
- d. Provide unique insights and actionable responses to tactical, cultural, political, economic, and social trends potentially affecting operations to counter and deter WMD, improvised threats, and threat networks in any CCMD AOR.
- e. Develop and deliver **Red Team Analysis, Findings, and Recommendations (Section F, Deliverable 51)** to emulate the threat using the User-Defined Operational Picture (UDOP), and other media as directed.
- f. Identify emerging issues/challenges within any CCMD AOR.
- g. Provide problem solving expertise in the CCMD AORs including the ability to integrate concepts/analysis from outside advisors
- h. Lead and conduct creative role-playing and war-gaming activities designed to understand various threat groups.
- i. Provide gap analyses (**Section F, Deliverable 50, Red Team/Wargame Scenarios/Reports**) that challenge the common assumptions and examine second- and third-order effects of plans for scenario development
- j. Deploy for short periods of time to required AORs to support Red Teams/war-game exercises as the mission dictates.
- k. Organize and conduct detailed seminars to enhance the knowledgebase of the Red Team.
- l. Assist the Government in designing scenarios to be employed in SIE computer simulations to emulate the threat.

**C.5.6.2 SUBTASK 2 – STRATEGIC INTERPLAY EXPLORATION (SIE)**

The contractor shall operate the SIE system to immerse analysts and pre-deployment leadership personnel into the target AOR environments using potential scenarios to develop understanding and practice in operating within a foreign culture and environment. This includes, but is not limited to, development and application of automated tools and techniques, development of scenarios and scripts, development of a robust lessons learned program (from previous sessions as well as in-theater live operations), and injection of research and analysis conducted under this TO. This system shall support unclassified and multi-level security operations up to the Secret level, when required. Any development activities shall be approved in advance by the Government.

**C.5.6.2.1 SUBTASK 6.2.1 – STRATEGIC INTERPLAY EXPLORATION (SIE)  
SYSTEM LIFECYCLE MANAGEMENT**

Access to and use of the SIE system will be provided to the contractor. The contractor shall use the SIE system to conduct alternative analyses by cultural, academic, war game, and threat team experts in an enhanced role playing simulation environment. The contractor shall ensure that adequate space, power, and security are available to accommodate the SIE hardware, software, and associated equipment.

The contractor shall maintain and implement an **SIE Life Cycle Management Plan (LCMP)** (Section F, Deliverable 52) and provide periodic **SIE System Status Reports** (Section F, Deliverable 53) to ensure that the system is updated in a timely and cost-effective manner, as approved by the FEDSIM COR in coordination with the DTRA TPOC.

The contractor shall ensure that updates and configuration of hardware and software fully support all SIE system requirements. The contractor shall perform configuration management of the SIE system and maintain records of hardware and software versions and other system documentation as requested.

The contractor shall maintain all hardware and software associated with the SIE system, including hardware refreshes, patches, and software updates in accordance with DoD instructions (DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)). Maintenance includes software updates for the correction of software defects (“bugs”), enhancements and modifications to improve the interface with simulation participants, operating system updates, and changes to ensure continued compatibility of the SIE system components. The contractor shall prepare all RMF authorization documentation in the DoD’s enterprise Mission Assurance Support Service (eMASS) as required to support authorization decisions and as directed by DTRA’s cognizant Information Systems Security Manager and Authorizing Official.

The contractor shall update and provide **SIE Certification and Accreditation Package Support** (Section F, Deliverable 54) to DTRA and Defense Security Systems (DSS) for system and site inspections and reviews.



## SECTION C - PERFORMANCE WORK STATEMENT

The contractor shall safeguard all Government information and property provided for use in the performance of this TO including, but not limited to, those designated as unclassified sensitive, For Official Use Only (FOUO), Operations Security (OPSEC) sensitive, and Privacy Act Information, in accordance with applicable Government directives.

### **C.5.6.2.2 SUBTASK 6.2.2 – STRATEGIC INTERPLAY EXPLORATION (SIE) OPERATION**

The contractor shall operate the SIE system and develop mission-focused scenarios that will be executed by Government simulation participants in an enhanced role playing exercise.

The contractor shall produce a **Simulation Session Record** for all simulation sessions (**Section F, Deliverable 55**), which shall include captured sound and/or images in a permanent form that is suitable for reproduction, all of the role-play interactions, text communications, images and videos. The record shall include a summary of group discussions conducted during each session. The record shall be included in an **SIE Theater Operational Planning Report (Section F, Deliverable 56)**, that responds to theater operational planning and anticipates second- and third-order effects of an adversary's adaptation of WMD and improvised threats in terms of the OE with alternative analysis by cultural, academic, and Red Team SMEs.

### **C.5.6.2.3 SUBTASK 6.2.3 –SCENARIO DEVELOPMENT AND POTENTIAL OUTCOMES**

The contractor shall develop mission-focused exercise scenarios (Strategic Interplay Exploration (SIE)) that will be executed by Government participants in an enhanced role playing exercise. The scenario development also supports **Section C.5.6.1** (Red-Teaming/War-gaming).

The contractor shall generate the threat analysis and enable the manipulation of virtual real-time war gaming scenarios and strategies similar to those executed by insurgent terrorist networks, social/political groups, and Commanders on the Ground through the simulation system. The contractor shall provide tools that capture the actions, reactions, and decisions of the Government role players' (Red/Green Teams) response to Blue Team operations, and provide dynamic output of the simulation session that may be delivered directly to the warfighter.

Scenarios developed shall:

- a. Provide participants the freedom to improvise (within the scenario guidelines) their choices and shape the direction and outcome of the simulation/scenario.
- b. Ensure scenario descriptions identify the goals of the session and include important historical information, capabilities, and available equipment.
- c. Install, operate, monitor, and maintain simulation computer workstations and networks in support of simulation-based events.
- d. Coordinate, resource, implement, and provide feedback for simulation exercises hosted at the contractor facility.

## SECTION C - PERFORMANCE WORK STATEMENT

- e. Conduct assessments and capture the effectiveness of the simulation scenarios as well as reactions by role players and leaders and provide a **Scenario Assessment/Effectiveness Report (Section F, Deliverable 57)**.
- f. Write scenarios that promote creativity in realistic decision making alternatives.
  - 1. Scenarios may be scripted and have minimal participation from the Scenario Master or have more interaction for the Scenario Master to author the simulation as required (combination of scripted and interactive segments).
  - 2. Potential injects from the Scenario Master during interactive segments may include visual representation of decisions made by the participants, changing actions made by the Blue Team (friendly forces), social events, political events, and other unpredictable events.
  - 3. Allow for the ability to adapt the scenario during the session through the interjection of videos, television shows, web videos, pictures, graphics, texts, etc.
- g. Provide a **Scenario Plan of Action (Section F, Deliverable 58)** for the Scenario Master for each session.
- h. Be capable of development and creation of **Scenario Potential Outcome Videos/Briefings (Section F, Deliverable 59)** that shall:
  - 1. Be no longer than 15 minutes in length and document the potential outcomes of the Red Team's actions.
  - 2. Depict lessons learned.
  - 3. Use broadcast quality.
  - 4. Be free of contractor copyright/trademark or other intellectual property markings.
  - 5. Enable playback of the video on standard computer readable media players supporting Compact Disk (CD)/Digital Versatile Disk (DVD) capabilities or be able to be compressed for secure email transmission and playback of the media file.

### **C.5.6.3 SUBTASK 3 – PROVIDE SIGNATURES ANALYSIS**

Signatures analysis is a specialized type of information gathering that serves to detect, track, identify, or describe the distinctive characteristics or signatures of a fixed or dynamic target. Often this can include gathering information about the capabilities of threat networks in radar, acoustic, or CBRNE areas. The contractor shall employ signature analysis based on environmental information to predict the likely behavior of human enemy networks. Typical problem sets include the analysis of unique terrain features, route analysis, WMD and improvised threat activity/events, caching of WMD and improvised threats, facilitation to produce WMD and improvised threats, WMD and improvised threat production, and support of ISR requirements.

Where possible, the contractor shall use Government Off-the-Shelf (GOTS) tools to conduct this type of analysis (i.e., ThreatMapper). If, through analysis, it is determined that GOTS tools are not suitable for the analysis required; the contractor may suggest alternate tools/technologies for analysis and predictive modeling. All suggested tool(s) shall meet DTRA software security protocols. The contractor shall approval from the FEDSIM COR in coordination with the DTRA

## SECTION C - PERFORMANCE WORK STATEMENT

TPOC, prior to adopting and/or using alternate tools for analysis. If a Commercial Off-the-Shelf (COTS) tool is approved for use by the FEDSIM COR and DTRA TPOC, the tool shall be used and maintained in accordance with DTRA software security protocols.

The contractor shall provide the following:

- a. Provide expertise in the application of signature analysis to analyze, understand, and exploit the advanced signals that enemy targets use to communicate.
- b. Determine the characteristics of a location that is associated with activities of a human enemy network.
- c. Analyze physical characteristics as requested to support the RFS process (**Section F, Deliverable 28, RFS Reports**) or to focus on Named Areas of Interest (NAIs).
- d. Establish predictive insights into likely enemy activity within an NAI that will help focus other analytical efforts, ISR, targeting, and tactical operations to anticipate enemy reactions and adaptations.
- e. Develop geospatially oriented analysis reports of threat activity based on a range of previously observed and evaluated physical signatures and information reporting.
- f. Participate in technical meetings to fuse analysis with other reports.
- g. Present analytical assessments derived from signature analysis to the DTRA and to other forums as required.
- h. Deliver UDOP overlays depicting threat activity based on previously observed and evaluated physical signatures.

The contractor shall prepare and deliver **Signature Analysis Reports (Section F, Deliverable 60)** that describe the analysis that was conducted and the predictions that were made.

### **C.5.6.4 SUBTASK 4 – PROVIDE GEOINT/IMINT/MASINT**

GEOINT analyzes the aerial and ground-permanent record imagery or other imagery products developed by photographic and electronic means to obtain information, determine target coordinates for accurate location of imagery research and analysis findings, identify enemy weapons and equipment defenses, assess installations and lines of communication, assess land and sea areas that could become battlegrounds in time of war, and recommend the use of imaging sensors for reconnaissance and surveillance missions.

GEOINT serves to exploit and manipulate geospatial data in complex graphics, textural reports, and briefings in order to create GEOINT reports such as shape files, geo-databases, .kml files and .kmz files for use with both ArcGIS and Google Earth, and to apply geospatial analytical methods, including the production of geospatial datasets and visualizations of geospatial information for customer-specified directed research, analysis, and reporting.

IMINT collects information via images (e.g., satellite and aerial photography). GEOINT and IMINT are complimented by the non-imaging MASINT collection which uses output from electro-optical and radar sensors.

## SECTION C - PERFORMANCE WORK STATEMENT

The contractor shall analyze and incorporate GEOINT, IMINT, and MASINT to respond to **RFS(s) (Section F, Deliverable 28, RFS Reports)** and to provide **GEOINT/IMINT/MASINT Reports (Section F, Deliverable 61)**. The contractor shall:

- a. Provide specialized expertise in geospatial MASINT analysis to retrieve, produce, and exploit standard and non-standard MASINT analyses.
- b. Provide specialized expertise in Geospatial IMINT to analyze aerial and ground-permanent record imagery or other imagery products developed by photographic and electronic means to obtain information to determine target coordinates for accurate location of imagery research and analysis findings.
- c. Support GEOINT/IMINT/MASINT KM/data curation (**Section C.5.5.7**) efforts by ensuring products are standardized. This includes, but is not limited to:
  1. Standardized data tagging and standardized report/analysis formats for responses to RFS (**Section F, Deliverable 28, RFS Reports**).
  2. Recommending the use of/or improvement to templates supporting the KM/data curation efforts.

### **C.5.6.5 SUBTASK 5 – PROVIDE THREAT FINANCE ANALYSIS**

Threat finance analysis is a component of specialized information gathering which looks at the economic aspects of human-induced insecurity, such as terrorism or organized crime. The integration of global financial systems as well as technological innovation and proliferation has reduced barriers to threat financing and money laundering, making it difficult to detect and disrupt such operations.

The contractor shall provide **Threat Financial Assessments/ Reports (Section F, Deliverable 62)** that fuse financial and transactional data from formal banking systems, financial reports, and/or other forms of reporting or information. The contractor shall provide assessments that address defense analytic requirements, may focus on specific target threat countries or events, and may include, but are not limited to the following:

- a. Identifying Threat financiers, facilitators, and financial networks/operations associated with terrorism, CWMD, counterintelligence, insurgency, proliferation, and operational activities which threaten U.S. national security interests.
- b. Processing and exploiting financial data through fusion methods and pattern analysis including flow analysis, network analysis, and statistical analysis.
- c. Assisting with performing financial forensic exploitation to identify and extract threat networks' finance data that is publicly available or contained in seized media.
- d. Identifying and extract relevant data, reflecting threat financial signatures. Identify collection gaps to guide further collection efforts.
- e. Performing finance network analysis, including fusing transactional data from all sources, including law enforcement, financial crimes enforcement network, SIGINT source, HUMINT collection, and open sources to understand payment relationships, revenue-generation, and money laundering methods.

## SECTION C - PERFORMANCE WORK STATEMENT

- f. Mapping of threat finance network activities and identify actors and methods for inclusion in finished **Threat Financial Assessments (Section F, Deliverable 62)**.

### **C.5.6.6 SUBTASK 6 – PROVIDE OPEN-SOURCE (OSINT) ANALYSIS**

OSINT is data collected from publicly available sources and Publicly Available Information (PAI). The contractor shall apply in-depth knowledge to identify emerging substantive issues within the focus AOR and succinctly communicate findings to the requesting customer by generating open-source assessments which provide a real-time situational understanding of threat networks employing or facilitating the use of WMD and improvised weapons in areas where U.S. collection capabilities are limited or data is unavailable.

The contractor shall provide an open-source analytical capability that provides real-time situational understanding of threat networks employing or facilitating the use of WMD and improvised weapons in areas where U.S. collection capabilities are limited or data is unavailable. The contractor shall use open source tools to passively collect, organize, analyze, and report on publicly available, unclassified, open source data. The contractor shall provide open-source/social media reporting to support the HUMINT disciplines, using only passive, non-intrusive techniques and COTS tools and information sources. Reporting shall effectively detect, assess, analyze, and report on social media trends, events, and key communicators. Analysis shall provide insight on cultural, political, economic, and social trends potentially affecting operations to counter and deter WMD, improvised threats, and threat networks in the AOR or for selected CCMD(s) (e.g., Africa Command (AFRICOM), and USCENTCOM). Cultural analysis may focus on native proficiency in languages such as, but not limited to, Arabic, Dari/Farsi, or Pashtu, as well as English proficiency. The contractor shall provide research and analysis with relevant operational targeting and management.

The contractor shall analyze and incorporate PAI to respond to **RFS(s) (Section F, Deliverable 28, RFS Reports)**. In support of OSINT, the contractor shall:

- a. Provide and produce in-depth analysis of the Area of Operation (AO) and Areas of Interest (AOIs).
- b. Use the analysis to produce associated OSINT reports including briefings and presentation materials (**Section F, Deliverable 63, OSINT Briefings/Materials**) to assist with the development of short/long-term strategic plans.
- c. Provide offsite analysis of surface, deep, and dark web content using passive research techniques. Include big data analytics and commercially available data sets as required to respond to RFS(s) (**Section F, Deliverable 28, RFS Reports**).
- d. Employ both purpose-built, customer-tailored tools and best practices developed to systematically examine and integrate traditional and non-traditional data sets.
- e. Provide output that will be targeted and fused with analytical reports on virtual source networks, trends, indicators and warnings, and finished reports that contribute to counter-improvised threat and CWMD operations against state and non-state threat networks.

#### **C.5.6.7 SUBTASK 7– PROVIDE CRITICAL FACTORS ANALYSIS**

The contractor shall provide expertise in critical factors analysis that supports military operations to counter and defeat WMD and improvised threats. Specifically, the contractor shall:

- a. Conduct critical factors analysis to identify centers of gravity related to operations to counter and deter WMD, improvised threats, and threat networks.
- b. Based upon critical factors analysis, identify targets of opportunity to disrupt WMD and improvised threat operations, including the sourcing, production, delivery, and placement of weapons.
- c. Deliver and coordinate **Critical Factors Reports (Section F, Deliverable 64)** that respond to RFSs for critical factors analysis.

#### **C.5.7 TASK 7 – PATTERN ANALYSIS/TECHNICAL SUPPORT**

Pattern Analysis provides direct support to a broad spectrum of customers to include military forces at tactical, operational, and strategic levels, as well as senior leaders. The contractor shall provide the pattern analysis software package of its choosing. The contractor shall provide all **Pattern Analysis Reports (Section F, Deliverable 65)** to the Government.

The contractor shall:

- a. Operate, manipulate, and manage large-scale data efforts relating to Geographic/Geospatial Information Systems (GIS), with particular emphasis on ArcGIS and Google Earth systems.
- b. Support pattern analysis methods and formulation of CoAs to operational commanders based upon exploiting patterns in the current theater of operations.
- c. Provide support in analyzing the effectiveness of DTRA initiatives, investment decisions, and dynamics of the WMD and improvised threat fight, operational modeling, and portfolio management.
- d. Provide traditional pattern and non-conventional pattern analysis.
- e. Understand criminal and other forms of predatory and terrorist behaviors and advanced knowledge of spatial statistics, time series techniques, and mathematical principals required for developing, implementing, and explaining scientific modeling and spatiotemporal behaviors.

#### **C.5.7.1 SUBTASK 1– PROVIDE DEPLOYED PATTERN ANALYSIS SUPPORT**

The contractor shall establish and maintain a capability to forward deploy Pattern Analysts that will embed with Government personnel. The contractor shall prepare newly assigned Pattern Analysts for a deployment. The contractor shall ensure that deployed Pattern Analysts are familiar with CWMD and counter-improvised threat databases and, analytical tools to include geospatial tools (ArcGIS, Google Earth). Pattern analysts shall have expertise in quantitative and qualitative techniques.

Specifically, the contractor shall:

## SECTION C - PERFORMANCE WORK STATEMENT

- a. Prepare and update **Pattern Analysis Training Materials (Section F, Deliverable 66)** to ensure newly assigned Pattern Analysts gain an understanding of key analytic tools, procedures, and methodologies used in theater and within the CCMD.
- b. Schedule, coordinate, and track training requirements with DTRA.
- c. Coordinate reach-back and reach-forward analysis with appropriate DTRA representatives and reach-back analysts.
- d. Work with embedded staff at CCMDs to provide recent, relevant theater analysis and data to support pattern analysis, strategic assessments, and other analysis as directed by the supported staff.

### **C.5.8 TASK 8 – OPERATIONS RESEARCH/SYSTEMS ANALYSIS (ORSA)**

The ORSA team provides a unique skill set that integrates military knowledge and experience with mathematics, statistics, quantitative analysis, and other scientific techniques to effectively solve a wide array of complex problems. The ORSA team manages large quantities of data, translate data into useful insights, and develop strategies and metrics in order to provide on-site tactical, operational, and strategic CoAs to senior leaders and decision-makers. The ORSA team provides leaders with actionable insights from data-driven analysis of operations, processes, and capabilities to identify trends, inform assessments of effectiveness, and mitigate risk.

The ORSA team supports a full range of exercises that are deployed/embedded with units in theater. The ORSA team deploys with the full reach-back capabilities. Reach-back offers greater resources when the complexity or scope of a given problem exceeds deployed ORSAs' capabilities. Additionally, the ORSA team supports DTRA by identifying significant WMD, improvised threat, and threat network trends and provides predictive analysis of enemy-initiated attacks to assist in planning. The contractor shall develop **ORSA Analysis Reports (Section F, Deliverable 67)** in accordance with the RFS request process.

#### **C.5.8.1 SUBTASK 1– PROVIDE DEPLOYED OPERATIONS RESEARCH/SYSTEMS ANALYSIS (ORSA) SUPPORT**

The contractor shall provide ORSA analysis services in support of current operations in deployed locations. Contractor ORSA analysis services shall include, but are not limited to:

- a. Provide technology assessment and integration for ORSA teams.
- b. Provide operational support including mining and analyzing CWMD and improvised threat data to identify and categorize trends as an element of supported forces.
- c. Produce CWMD and Improvised Threat Quantitative Analytical Reports (**Section F, Deliverable 67, ORSA Analysis Reports**), operational trend assessments, and analyses.
- d. Produce analysis of unit operations using operations research techniques.
- e. Facilitate reach-back analysis with DTRA, as required.
- f. Work with embedded staff, such as Operations and Analysis Officers and data collectors.
- g. Facilitate data transfer from theater to CONUS.
- h. Perform causality assessment and mitigation analysis.

## SECTION C - PERFORMANCE WORK STATEMENT

- i. Provide analysis support to units in mission training events, readiness exercises, and pre-deployment rehearsals.
- j. Provide geospatial analysis and reporting (**Section F, Deliverable 67, ORSA Analysis Reports**).

### **C.5.8.2 SUBTASK 2– PROVIDE DEPLOYED OPERATIONS RESEARCH/SYSTEMS ANALYSIS (ORSA) TRAINING SUPPORT**

The contractor shall establish and maintain a current deployed ORSA training program to prepare newly assigned ORSAs for a deployment with forward-deployed units. Training shall include CWMD and counter-improvised threat database familiarization, practical use of analytical tools to include geospatial tools (ArcGIS, Google Earth), quantitative and qualitative techniques, and an introduction to the AO as it pertains to CWMD and improvised threats. Training services shall include ORSA support to units and staff during deployment exercises at designated locations CONUS and OCONUS in Government-owned facilities. Specifically, the contractor shall:

- a. Prepare and update **ORSA Training Materials (Section F, Deliverable 68)** to ensure newly assigned ORSA Teams gain an understanding of key analytic tools, procedures, and methodologies used in theater.
- b. Schedule, coordinate and track training requirements with DTRA.
- c. Provide units undergoing mission readiness training with tailored research and analysis products, trend assessments, and analysis of unit operations based on recent and unique ORSA techniques used currently in theater.
- d. Coordinate reach-back and reach-forward analysis with appropriate training event representatives and participants.
- e. Work with embedded staff at training events to provide recent, relevant theater analysis and data to support mission readiness, combat training, and designated pre-deployment events.

### **C.5.8.3 SUBTASK 3 – ON-SITE OPERATIONS RESEARCH/SYSTEMS ANALYSIS (ORSA) SUPPORT**

The contractor shall provide ORSA and geospatial analysis to support operations analysis teams, social analytical teams, and special operations analytical teams. This support includes providing actionable insight reporting from data-driven analysis of operations, processes, and capabilities to identify trends, inform assessments, and mitigate risk to minimize the impact of WMD and improvised threats. The contractor shall:

- a. Provide expertise in data mining, statistical analysis, causal analysis, and geospatial analysis, integrate multiple disciplines in an ORSA team to translate applicable methods into language and application understandable by operational commanders who are in a current theater of operations.
- b. Maintain data extraction to support assessments, providing modifications, updates, and new metrics as required.



## SECTION C - PERFORMANCE WORK STATEMENT

- c. Automate the collection, parsing, and mining of large datasets from different data sources.
- d. Provide DTRA leadership with quantitative organizational assessments to support functional evaluations (**Section F, Deliverable 67, ORSA Analysis Reports**).
- e. Provide unstructured text processing and analysis and/or use network analysis methodologies to support the DTRA mission.
- f. Perform geospatial CWMD and improvised threat assessments by gathering input from the appropriate CCMDs and other U.S. Government organizations.
- g. Identify alternatives and consequences on a wide variety of CWMD and counter-improvised threat-related geospatial trends.
- h. Assist in the development of forecasting techniques, analyzing trends, and developing geospatial products and tools, present analytical results to a military audience, and provide CoAs that will enhance the development of forecasting techniques and approaches that will enable the detection of geospatial trends and patterns for predictive assessments.
- i. Review research and analyses involving a spatial context of WMD and improvised threats in support of DTRA and monitor efforts highlighting the strengths, weaknesses, and areas that may prove to be the source of actionable CoAs for DTRA senior leaders.

### **C.5.9 TASK 9 – JOINT EXPEDITIONARY TEAM (JET)**

The JET provides analytical expertise in all aspects of CWMD and counter-improvised threat operations to support U.S. forces, (combat and non-combat) worldwide. The contractor shall gather information, conduct quick-look assessments, provide expertise to deployed U.S. forces, conduct unit debriefings of re-deploying U.S. forces, participate in training missions and pre-deployment activities, and assist DTRA with information exchanges with partner nations. The contractor shall inform DTRA leadership on CWMD and counter-improvised lessons learned and the effectiveness of quick-look assessments. Results of any analysis shall be documented in **JET Technical Analysis Reports (Section F, Deliverable 69)**, unless otherwise specified. The contractor shall facilitate the certification and qualification of the warfighter on selected COTS and GOTS Unmanned Aerial Systems (UAS).

#### **C.5.9.1 SUBTASK 1 – INFORM AND SUPPORT PRE-DEPLOYMENT TRAINING**

The contractor shall support training missions involving U.S. forces preparing for combat deployments and contingency operations across the globe. Support may include the Combat Training Centers (CTCs), home station training on installations, test sites and areas, and integration of interagency entities into some training scenarios. Contractor support shall include but is not limited to; requirements analysis, assessments, and development of training requirements enabling the fusion of analysis operations, and material/non-material solutions in support of the counter-improvised threat and CWMD mission. The contractor shall provide CWMD and counter-improvised threat training support to Mission Rehearsal Exercises and unit Battle Staff training as required. The contractor shall maintain awareness of emerging CWMD and counter-improvised threat technologies and initiatives. The contractor shall support

## SECTION C - PERFORMANCE WORK STATEMENT

operations research personnel in conducting CWMD and counter-improvised threat training support initiative assessments as required by the Government.

The contractor shall provide pre-deployment analysis for U.S. forces preparing for combat missions and contingency operations across the globe. This support includes, but is not limited to, training, exercise deployment and execution, analysis, and sharing of lessons learned. Each site aligned with pre-deployment activities shall mirror the composition of the team of the intended deployment. This support may be provided at the Brigade-level at home station, training installations, and test sites or areas, and may include integration of interagency entities into training scenarios. Duty locations include DTRA Headquarters within the NCR and CCMD headquarters as indicated in the RFS. Specific locations will be determined based on rotation requirements. The contractor shall:

- a. Attend pre-deployment training on evolving subjects related to operational planning.
- b. Develop and produce analyses, assessments, and training requirements that enable the fusion of analysis, operations, and material/non-material solutions in support of counter-improvised threat and CWMD (**Section F, Deliverable 69, JET Technical Analysis Reports**).
- c. Identify, plan, and execute pre-deployment actions necessary to ensure smooth future deployment and reach-back.
- d. Plan for and participate in pre-deployment exercises and war-games, such as (but not limited to) Mission Rehearsal Exercises, Field Training Exercises, and Command Post Exercises.
- e. Participate in data collection, reporting, and interview activities to develop operational assessments.

### **C.5.9.2 SUBTASK 2 – EMBED WITH OPERATIONAL UNITS**

The contractor shall embed with DTRA personnel and provide analysis of CWMD and counter-improvised threats in deployed environments. The contractor shall:

- a. Provide CWMD and counter-improvised threat training analysis to U.S. forces before and after deployments.
- b. Analyze TTPs to provide DTRA with best practices and effective solutions to WMD and improvised threat challenges.
- c. Conduct research and analysis that considers all OEs across the range of military options and joint campaign continuum.
- d. Conduct analysis by observing, collecting, developing, validating, and disseminating, emerging friendly force and enemy CWMD and counter-improvised threat TTPs.
- e. Assist DTRA with the identification, training, and integration of enduring and emerging CWMD and counter-improvised threat technologies.
- f. Provide CWMD and counter-improvised threat support to DTRA.
- g. Provide analysis in response to RFS (**Section F, Deliverable 28, RFS Reports**).

## SECTION C - PERFORMANCE WORK STATEMENT

### **C.5.9.3 SUBTASK 3 – DEPLOY TO AREA OF RESPONSIBILITY (AOR)**

The contractor shall deploy to the current theater of operation for 90-120-day periods to inform and assist organizations by enhancing the situational awareness, identifying critical capability gaps, and improving CWMD and counter-improvised threat material/non-material solutions, systems, processes, initiatives, and strategies. The contractor shall:

- a. Embed with DTRA and CCMDs to provide analysis that will facilitate the execution of their operational missions. Analysis provided shall include, but is not limited to OE shaping and management, full-spectrum operations (offense, defense, stability, and civil support), irregular warfare, Counterinsurgency (COIN), CT, and training support.
- b. Observe and collect **First-Hand CWMD and Counter-Improvised Threat-Related Information (Section F, Deliverable 70)**, then analyze and disseminate current and relevant friendly or enemy TTPs, lessons learned, and best practices to the CWMD and counter-improvised threat Community of Action (i.e., operational military and Special Operation Forces (SOF) elements, Federal agencies, academic institutions, and training centers).
- c. Provide research and analysis support to the CTCs, units on installations, test sites, and areas, interagency groups, and training commands in the areas of; fusion of analysis, operations, and material/non-material solutions in support of CWMD and counter-improvised threat mission.
- d. Assist supported unit(s) throughout pre-deployment training and exercise phases in all aspects of CWMD and counter-improvised threat plans and operations.
- e. Integrate counter-improvised threat framework and methodologies, tactical and technical countermeasures, and TTP(s) to deploying/deployed units.

### **C.5.9.4 SUBTASK 4 – PROVIDE NON-STANDARD SPECIALIZED COUNTER-WMD (CWMD) AND COUNTER-EMERGING IMPROVISED THREAT SUPPORT**

DTRA is the DoD's leader on CWMD and counter improvised threats. As such DTRA supports CWMD and improvised threat exchange events with U.S. Forces, partner nations, and other Government agencies. The contractor shall provide analysis of emerging and improvised threats to DTRA in order to support exchange events. Contractor personnel may be required to accompany and support DTRA personnel that present CWMD and counter improvised threat analysis at exchange events. These exchange events may occur at CONUS or OCONUS locations and the subject of the exchange event (and the required analysis) may depend on the need of the event attendees. The contractor shall assist and provide input for the continued refinement and development of outlines and expertise support packages/reports in response to RFS (**Section F, Deliverable 28, RFS Reports**) as required to close gaps in knowledge and experience in response to emerging threats.

The contractor shall:

- a. Provide information/analysis to facilitate awareness of CWMD and counter-improvised threat.
- b. Provide information/analysis on strategies to defeat improvised-threat defeat.

## SECTION C - PERFORMANCE WORK STATEMENT

- c. Support Government testing of improvised-threat detection equipment.
- d. Provide training and support for Counter-Unmanned Aircraft Systems (C-UAS).
- e. Provide information/analysis on sensitive Site Explosive Exploitation (SSE).
- f. Provide CWMD training courses.

### **C.5.9.5 SUBTASK 5 – PROVIDE SMALL UNMANNED AIRCRAFT SYSTEM (UAS) FLIGHT SAFETY AND STANDARDIZATION QUALIFICATION/CERTIFICATION PROGRAM SUPPORT**

The contractor shall assist DTRA with maintaining the Small UAS Flight Safety and Standardization Program. The contractor shall update and maintain the qualification and certification standards for U.S. Government Personnel on various COTS and GOTS small UAS in accordance with the Office of the Secretary of Defense (OSD), DoD Policy Directives, and the DTRA Air Force Special Operations Command (AFSOC) Letter of Agreement (LOA). Contractor personnel supporting this task shall be qualified and certified in accordance with AFSOC Air Force Manual (AFMAN) 11-502. Specifically the contractor shall:

- a. Assist the DTRA Safety Office with conducting periodic UAS flight safety risk assessments.
- b. Observe, identify, and share UAS flight safety lessons learned and best practices with the DTRA and DTRA's supported UAS communities.
- c. Assist DTRA with the coordination and synchronization of information between DTRA Divisions and AFSOC Program Management Office (PMO).
- d. Support DTRA's UAS mission by ensuring the timely qualification and certification of Government personnel required to operate UAS in CONUS and OCONUS locations.

### **C.5.9.6 SUBTASK 6 – PROVIDE LOGISTICS SERVICES**

The contractor shall support the Government with the receipt, shipping, handling, and inventory, materials and supplies that support deployment of personnel to OCONUS operations. The contractor shall create and maintain an official record of **assets** in an inventory system and track the assets within DTRA's Integrated Logistics System (ILS) (**Section F, Deliverable 71 Asset Inventory**). This includes maintaining accountability and tracking inventory distributed to DTRA personnel. The contractor shall consider the possible use of Government transportation and availability of U.S. flag shipping services where practicable.

In addition, the contractor shall:

- a. Maintain accountability and provide logistics/supply support expertise at Government facilities to assist DTRA with maintaining control of DTRA property.
- b. Maintain and update the **Asset Inventory (Section F, Deliverable 72)**.
- c. Provide on-site ILS support for DTRA teams as required.
- d. Provide maintenance support to the ILS system.
- e. Provide secure shipping support for analysis products.
- f. Provide shipping/tracking and accountability support for deployment-related supplies.

## SECTION C - PERFORMANCE WORK STATEMENT

### **C.5.10 TASK 10 – OPTIONAL SURGE**

The contractor shall provide surge support restricted to the requirements in Tasks 1-9 of the awarded TO. DTRA operates in a dynamic and evolving mission environment. It is anticipated that as a result of such an environment, augmentation of existing resources may be required in response to any global contingencies and CWMD/CTN. The purpose of this task is to allow TO capacity in support of DTRA requirements. Unpredictable world events demand that DTRA have the capability to provide deployed and additional support as required in CONUS, OCONUS, and HD/CZ. Additional support requirements are variable in length and LOE. Decisive efforts are defined as situations where U.S. forces are deployed in support of a contingency operation that is contested by threat networks and their use of improvised weapons. Support may be project based and result in a long-term increase of LOE. Support may require short-term TDY (e.g., one month) or longer-term deployments (e.g., one or more months). Requirements and deliverables for the additional support are described in Tasks 1-9 and are within the scope of this TO but require additional personnel to meet the requirement. When additional support is needed, the Government will exercise the optional surge support CLIN.